## CLAIMS

We claim:

1. A collaborative file rights management method comprising:

identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application;

suppressing said file I/O request;

automatically extracting digital rights management data appended to said file;

providing said file to said authoring application; and,

managing access to said file in said authoring application based upon said extracted digital rights management data.

2. The method of claim 1, further comprising:

decrypting said file.

3. The method of claim 1, wherein said extracting step further comprises:

determining environmental data associated with said file I/O request, said environmental data comprising at least one of a requestor's identity, a requestor's class, a requestor's computing domain, a requestor's location, a password, a time of day, and a date; and,

extracting an access policy appended to said file

4. The method of claim 3, wherein said providing step comprises:

comparing said access policy to at least a portion of said environmental data;

authenticating said file I/O request based upon said comparison; and,

providing said file to said authoring application only if said file I/O request has been authenticated.

5. The method of claim 1, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

6. The method of claim 1, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to access said file in one of said I/O request packets.

7. The method of claim 1, wherein said management step comprises:

intercepting operating system messages in said authoring application;

detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data; and,

quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

8. The method of claim 7, wherein said authoring application operations comprise operations selected from the group consisting of clipboard operations, printing operations, file saving operations, and file editing operations.

9. A collaborative file rights management method comprising:

identifying a file input/output (I/O) request to save a file, said request originating in an authoring application;

suppressing said request and automatically encrypting said file;

appending an access policy and digital rights management data to said encrypted file; and,

storing said file in fixed storage.

10. The method of claim 9, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

11. The method of claim 9, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to save said file in one of said I/O request packets.

12. A collaborative file rights management system comprising:

a file security management application configured to intercept operating system messages directed to an authoring application; and,

a file security filter driver configured to identify file input/output (I/O) requests received in a kernel-layer file system manager to open an encrypted file in said authoring application;

said file security filter driver quashing said file I/O requests, decrypting said encrypted file and providing said decrypted file to said authoring application;

said file security management application extracting digital rights management data appended to said encrypted file, detecting among intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights

management data, and, quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

13. A machine readable storage having stored thereon a computer program for managing digital rights in a collaborative file, said computer program comprising a routine set of instructions for causing the machine to perform the steps of:

identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application;

suppressing said file I/O request;

automatically extracting digital rights management data appended to said file;

providing said file to said authoring application; and,

managing access to said file in said authoring application based upon said extracted digital rights management data.

14. The machine readable storage of claim 13, further comprising:

decrypting said file.

15. The machine readable storage of claim 13, wherein said extracting step further comprises:

determining environmental data associated with said file I/O request, said environmental data comprising at least one of a requestor's identity, a requestor's class,

a requestor's computing domain, a requestor's location, a password, a time of day, and a date; and,

extracting an access policy appended to said file

16. The machine readable storage of claim 15, wherein said providing step comprises:

comparing said access policy to at least a portion of said environmental data;

authenticating said file I/O request based upon said comparison; and,

providing said file to said authoring application only if said file I/O request has been authenticated.

17. The machine readable storage of claim 13, wherein said suppressing step comprises:

posting a responsive message to said authoring application;

intercepting an operating system event in said authoring application, said operating system event indicating receipt of said responsive message; and,

quashing further processing of said intercepted operating system event.

18. The machine readable storage of claim 13, wherein said identifying step comprises:

monitoring kernel-level file I/O requests contained in I/O request packets processed in a file system manager; and,

detecting said file I/O request to access said file in one of said I/O request packets.

19. The machine readable storage of claim 13, wherein said management step comprises:

intercepting operating system messages in said authoring application;

detecting among said intercepted operating system messages, operating system messages directed to authoring application operations which can be limited according to digital rights specified in said extracted digital rights management data; and,

quashing said detected events where said digital rights management data prohibits execution of said authoring application operations.

20. The machine readable storage of claim 19, wherein said authoring application operations comprise operations selected from the group consisting of clipboard operations, printing operations, file saving operations, and file editing operations.